IN THE CLAIMS

Kindly amend claims 1, 3, 5 and 6 as shown in the following claim listing:

1. (currently amended) A network apparatus (2) for communicating with a network (A) and comprising
   - a biometry module (3) for detecting biometrical data of a user (1); said biometrical data of a user (1) also being supplied to said network (A);
   - a configuration module (4)directly coupled to said biometry module (3) which is adapted to determine an unambiguous network identifier and/or an unambiguous initial key from biometrical data provided by the biometry module (3) for ~~the~~ an encrypted communication ~~(particularly~~ , such as in the configuration phase~~)~~ , with a second apparatus.

2. (original) An apparatus as claimed in claim 1, characterized in that it is adapted to eliminate the biometrical data of a user (1) after their use by the configuration module (4).

3. (currently amended) An apparatus as claimed in claim 1, characterized in that the communication with the second apparatus takes place in a wireless or wired way, ~~particularly~~ such as via a power supply mains.

4. (previously presented) An apparatus as claimed in claim 1, characterized in that the configuration module is adapted to manage a list of biometrical data and/or data derived from said list for different users (1) of an authorized user group.

5. (currently amended) A method of assigning a network apparatus (2) to a network (A), wherein biometrical data of a user (1) are supplied to the network (A) and are also supplied to and detected by the apparatus (2) and an unambiguous network identifier is derived therefrom, which identifier is used and known in the network (A) from previous and/or simultaneous inputs of the same biometrical data.

6. (currently amended) A method of configuring a communication connection between a network apparatus (2) and a network (A), wherein biometrical data of a user (1) are supplied to the network (A) and are also supplied to and detected by the network apparatus (2) and an unambiguous initial key is derived therefrom, which initial key is known in the network (A) from previous and/or simultaneous inputs of the same biometrical data and is used for a secure communication ~~(particularly~~ , such as in the configuration phase).